REMARKS

Claims 1, 3-6, 8-10, 13-19 and 22-26 are all the claims pending in the application. The Examiner has withdrawn the objection to the drawings and the rejection of claims 1-8 under 35 U.S.C. § 101. Claims 1, 3-6, 8-10, 13-19 and 22-26 remain rejected on the prior art grounds of record.

I. Claim Rejection under 35 U.S.C. § 103(a) over U.S. Patent Appln. Publ. 2003/0051009 to Shah et al. ("Shah") in view of U.S. Patent No. 5,075,884 to Sherman et al. ("Sherman")

Claims 1, 3-5, 8-10, 13-19 and 22-25 remain rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Shah in view of Sherman.

A. Claim 1

Claim 1 recites,

> A network connection apparatus, comprising:
> a computer-readable medium storing a computer program, which when executed by a computer processor, comprises a join module for connecting a second network, to which the join module belongs, with a first network in response to an inter-network connection request message transmitted from the first network, setting a security level of the first network to a set security level, and controlling network command messages in response to the set security level;
> a connection module for receiving the inter-network connection request message transmitted from the first network and connecting the first network with the second network;
> an authentication/security module for determining whether to allow a connection of the first network that has transmitted the inter-network connection request message to the connection module, and setting and checking the security level of the first network; and
> a transmission module for transmitting a requested network command message requested by the first network when the connection is allowed by the authentication/security module;
> wherein the security level is applied differently depending on the first network to be connected.

In the Amendment filed April 7, 2008, Applicant argued that, in the network connection apparatus of claim 1, the authentication/security module determines whether the connection to the first network that transmitted the network-connection message between networks is to be allowed and sets and checks the security level for the network. Also, the security level is applied differently according to the first network that transmitted the connection-request message between networks. That is, if the first network that transmitted the connection-request message between networks is connected in the state where each level has been set in the device existing in its own network, the device to be connected to the first network and the device not to be connected to the first network are determined based on the set level. Hence, in the case of important devices, by setting the level high, when connected to the first network, only devices set low can be shown.

On the other hand, Applicant argued that Sherman is directed to a multi-level security workstation. Referring to FIG. 2 of Sherman, the workstation has a separate internal configuration such as a TCB, a port and a processor, and the security level information is stored in the TCB, the port and the processor. Hence, the configuration taught by Sherman is different from that of the apparatus described in claim 1. Applicant further argued that Sherman fails to teach or suggest the claimed features of setting the security level for the first network, and applying a different security level according to the network that transmits the connection-request message between networks. Specifically the Examiner cites col. 4, lines 33-41 and 60-61 of Sherman as teaching the claim feature of "setting a security level of the first network to a set security level, and controlling network command messages in response to the set security level." Sherman merely teaches that a "secure LAN 26 enables communication between nodes...of equivalent security levels in isolation from TCBs at other security levels thus preventing

communication between TCBs of nonequivalent security levels." *See* Sherman at col. 4, lines 36-41. Sherman also teaches that each port of a workstation has a defined security level which is specified by the TCB. *See* Sherman at col. 4, lines 60-63. In other words, Sherman merely teaches that ports of a workstation contain a security level and that communication between ports is restricted according to the security levels. However, Sherman does not teach or suggest "setting a security level."

In the present Office Action the Examiner responds that Sherman teaches that each port of the workstation 12 has a defined security level as specified by a TCB, which is coupled to a processor via a dedicated port. *See* Office Action at page 14; Sherman at Figure 1. The Examiner concludes that because a port can be used to communicate with other networks, specifying a security level of a port which communicates with another network sets the security level of the other network. Applicant respectfully traverses the rejection as follows.

Claim 1 recites, *inter alia* "a join module for connecting a second network, to which the join module belongs, with a first network in response to an inter-network connection request message transmitted from the first network, setting a security level of the first network to a set security level, and controlling network command messages in response to the set security level." In other words, when the first network transmits an inter-network connection request message to the second network, the join module, which belongs to the second network, sets a security level of the first network to a set security level. The Examiner relies on the TCBs taught by Sherman as teaching the setting of security levels. However, each TCB of Sherman only sets the security level of its corresponding port.

For example, referring to workstation 12 illustrated in Figure 1 of Sherman, TCB 20 sets the security level of port 14, and TCB 22 sets the security level of port 16. In this case, since

port 14 is connected to secret processor 42, the security level of port 14 is set to "secret." Since port 16 is connected to top secret processor 44, TCB 22 sets the security level of port 16 as "top secret." Because the ports 14 and 16 are set at different security levels, TCBs 20 and 22 cannot directly communicate. If TCB 20 wishes to communicate with TCB 22, it must do so through guard means 28 via TCB 30 ("secret" security level) and TCB 32 ("top secret" security level). *See* Sherman at col. 4, lines 49-55. That is, once each TCB has set the security level for its corresponding port, only ports having equal security levels may communicate directly.

Comparing the structure taught by Sherman to the claim language, the TCB of a second network that receives an inter-network connection request from a first network does not set the security level of the first network that sent the inter-network connection request message. For example, if a TCB having a security level of "secret" transmits a request for communication to a TCB having a security level of "top secret," the top secret TCB does not set the security level of the secret TCB to "top secret." Doing so would completely frustrate the objective of Sherman, which is to restrict communications between ports having different security levels. The Examiner's assertion that "because a port can be used to communicate with other networks, specifying a security level of a port which communicates with another network sets the security level of the other network," is completely contrary to the teachings of Sherman. Thus, Sherman actually teaches away from the apparatus of claim 1. *See* MPEP §§ 2141.02 and 2145.

Accordingly, Applicant submits that the teachings of Shah and Sherman, taken alone or in combination, fail to disclose or suggest all of the features of claim 1. Thus, Applicant submits that claim 1 is patentable over Shah and Sherman for at least the foregoing reasons.

B. Claims 3-5 and 8

Since claims 3-5 and 8 are dependent upon claim 1, Applicant submits that such claims are patentable over Shah and Sherman at least by virtue of their dependency.

C. Claims 9, 10 and 13-16

Since claim 9 recites features similar to those discussed above in conjunction with claim 1, Applicant submits that claim 9 is patentable over Shah and Sherman for at least similar reasons. Since claims 10 and 13-16 are dependent upon claim 9, Applicant submits that such claims are patentable over Shah and Sherman at least by virtue of their dependency.

D. Claims 18, 19 and 22-25

Since claim 18 recites features similar to those discussed above in conjunction with claim 1, Applicant submits that claim 18 is patentable over Shah and Sherman for at least similar reasons. Since claims 19 and 22-25 are dependent upon claim 18, Applicant submits that such claims are patentable over Shah and Sherman at least by virtue of their dependency.

II. Claim Rejection under 35 U.S.C. § 103(a) over Shah in view of Sherman, in further view of U.S. Patent No. 6,725,281 to Zintel et al. ("Zintel")

Claims 6, 17 and 26 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Shah in view of Sherman, in further view of Zintel.

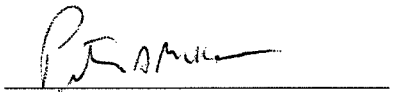
Since claims 6, 17 and 26 are dependent upon claims 1, 9 and 18, respectively, and Zintel fails to cure the deficient teachings of Shah and Sherman with regard to claims 1, 9 and 18, Applicant submits that claims 6, 17 and 26 are patentable over the cited references at least by virtue of their respective dependencies.

III. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,



Peter A. McKenna
Registration No. 38,551

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: September 9, 2008